UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/275,911	03/24/1999	ROBERT G. LIU	42390.P7033	1385

7590 09/30/2002

BLAKELY SOKOLOFF TAYLOR AND ZAFMAN
7TH FLOOR
12400 WILSHIRE BOULEVARD
LOS ANGELES, CA 90025

EXAMINER
BAUM, RONALD

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/30/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/275,911	Applicant(s) LIU ET AL.	
	Examiner Ronald Baum	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 35 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 35 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-35 are pending for examination.

2. Claims 1-35 are rejected.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 20 recites the limitation "other operands are each the processed key" in claim 16. There is insufficient antecedent basis for this limitation in the claim. Claim 20 is rejected.

4. Claim 21 recites the limitation "there are more than one level of XOR operations" in claim 16. There is insufficient antecedent basis for this limitation in the claim. Claim 21 is rejected.

5. Claim 35 recites the limitation "The method of claim 34". The examiner assumes that for the purpose of applying art, the claim preamble should recite "The system of claim 34", since this claim comprises the system elements of claim 34. Claim 35 is rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

6. Claims 1-3, 6, 12-17, 26-35 are rejected under 35 U.S.C. 102(b) as being anticipated by Faria, UK Patent Application GB 2316278A.

As per claims 1, 14, 26, 29, 32 and 34, Faria is directed towards a method of encrypting and subsequent decrypting sequences of bits (blocks of (streaming) data) comprising individually transforming (scrambling) the data blocks with a encryption key (page 2, lines 16-22). The user sends the server it's unique identity code (remote computer number), whereas the server also stores the audio and/or video data to be sent to the user (page 2, lines 27-38) as is done for MPEG audio and/or video.

Therefore, the Faria encryption/decryption (scrambling/de-scrambling) of data is done on a received data file block of data (digital video) using a key that is a function of the receiver (remote computer) unique identity (number) code (page 2, lines 27-36).

7. Claims 2, 15, 16, 33 and 35 additionally recite the limitation that the scrambling/de-scrambling key be processed from (i.e., a function of) at least, the remote computer number. Faria claim 10 recites using an encryption/decryption key that is a function of (only) the identity code. Claims 2, 15, 16 are rejected.

8. Claims 3, 6 and 17 additionally recite the limitation that logical exclusive OR'g (XOR) is used (an inherently 2 operand logical operation) to create scrambling/de-scrambling data from the data and the other operand, that being PK. Faria encrypts/decrypts by XOR of the data (1st

operand) and the keying (other operand) data (page 3, lines 4-43, page 4, lines 1-14). Claims 3, 6 and 17 are rejected.

9. Claims 27-28, 30-31 differs from claims 2-3 and 15-16 respectively in that articles instead of methods are recited. Faria clearly discloses articles in the form of servers and user workstations.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 4, 5, 18, 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Faria, UK Patent Application GB 2316278A , as applied to claims 3 and 17 above, and further in view of SCHNEIER, BRUCE, Applied cryptography, second edition, John Wiley & Sons, Inc. 1996, pages 193, section 9.3, 1st paragraph, IDS paper No. 4.

Faria is directed towards a method of encrypting and subsequent decrypting sequences of bits (blocks of (streaming) data) comprising individually transforming (scrambling) the data blocks with a encryption key (page 2, lines 16-22). The user sends the server it's unique identity code (remote computer number), whereas the server also stores the audio and/or video data to be sent to the user (page 2, lines 27-38) as is done for MPEG audio and/or video.

Therefore, the Faria encryption/decryption (scrambling/de-scrambling) of data is done on a received data file block of data (digital video) using a key that is a function of the receiver (remote computer) unique identity (number) code (page 2, lines 27-36).

Faria does not teach the use of data chaining of any given block of data with data from a previous block.

Schneier teaches that chaining adds feedback to block cipher: "The results of the encryption of previous blocks are fed into encryption of the current block..." (section 9.3, 1st paragraph). Also, where the feedback is the plaintext, Plaintext Block Chaining (PBC) is the encryption mode used (page 208, More Modes paragraph). In this case, the PBC initialization vector (page 194, Initialization paragraph) is the applicant's PK, and each subsequent feedback input to the XOR function is the previous plaintext (digital video data) block. The chaining is done to prevent block replay of ECB encrypted data blocks (section 9.2, last paragraph).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the data block chaining of Schneier to the XOR scrambling of data blocks of Faria to prevent block replay attacks on the data block stream (Schneier, section 9.2, last paragraph).

11. Claims 7, 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Faria, UK Patent Application GB 2316278A, and further in view of Hartman, Jr., U.S. Patent 5,224,166.

Claims 7, 25 additionally recite the limitation that the remote computer number is a processor number. Faria does not teach the use of a remote computer number being a function of a processor number.

Hartman teaches of the use of the remote processor's serial number being used for the remote data-requesting device accessing a media (data) provider (col. 4, lines 1-22) across a data communications path.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Hartman teachings of the use of the remote processor's serial number to the Faria encryption method in order to uniquely identify encryption and keying processing (col. 3, lines 1-28).

12. Claims 12, 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Faria, UK Patent Application GB 2316278A, and further in view of Hartman, Jr., U.S. Patent 5,224,166.

Claims 12, 13 additionally recite the limitation that the remote computer is uniquely authenticated and that authentication is a function of the remote computer number. Faria does not teach the use of the remote computer being a unique function of remote computer number.

Hartman teaches of the use of the remote processor's serial number being used for the remote data-requesting device authentication to the media provider (col. 4, lines 1-22, 35-45) across a data communications path.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Hartman teachings of the use of the remote processor's serial number for remote authentication to the Faria encryption method in order to uniquely identify encryption and keying processing (col. 3, lines 1-28).

13. Claims 8-11, 22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Faria, UK Patent Application GB 2316278A , and further in view of Dent, U.S. Patent 5,091,942.

Claims 8-11, 22-24 additionally recite the limitations that numbering of the digital video data blocks is determined and used as a component of the encryption/decryption key . Faria does not teach the use of the digital data blocks (data framing designation) being numbered.

Dent teaches of the use of a data frame to frame (block) determined number to generate the keystream data used for the stream encryption/decryption (col. 2, lines 67-68, col. 3, lines 1-14, col. 9, lines 16-22) via modulo-2 addition (XOR) operation (col. 11, lines 17-24).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Dent teachings of the use of data frame to frame (block) determined number to generate the keystream data used for the stream encryption/decryption (via the logical XOR operation on the operands) to the Faria encryption/decryption method for video/audio data streams. Dent describes how transmit to receive synchronization is a requirement for the communications to occur (col. 3, lines 3-10).

Conclusion

14. The examiner asserts that the claims are incomprehensible such that the examiner can't apply art at this time. If applicant would like an interview to discuss the rejection, he may contact the examiner at the number listed below to arrange a mutually convenient date and time.

15. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached at (703) 305-9711. The Fax numbers for the organization where this application is assigned are:

After-final (703) 746-7238

Official (703) 746-7239

Non-Official/Draft (703) 746-7246

Ronald Baum

Patent Examiner

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100